

Welcome to the PIA for FY 2011!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaaw.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to christina.pettit@va.gov to receive full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name:

Health Data Repository (HDR)

OMB Unique System / Application / Program Identifier

(AKA: UPID #):

029-00-01-11-01-1183-00

Description of System/ Application/ Program:

The Health Data Repository (HDR) is a data repository of clinical information that resides on one or more independent platforms and is used by clinicians and other personnel to facilitate longitudinal patient-centric care.

Facility Name:

AITC

Title:

Name:

Phone:

Email:

Privacy Officer:

Garnett Best

202-461-7474

garnett.best@va.gov

Information Security Officer:

Larry Skrabut

801-588-5208

larry.skrabut@va.gov

System/Chief Information Owner:

Joe Gibbons

518-449-0618

joe.gibbons@va.gov

Program Manager:

Gloria Smith

801-588-5052

gsmith@va.gov

Person Completing Document:

Analida Aguilar

512-326-6023

analida.aguilar@va.gov

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)

12/2009

Date Approval To Operate Expires:

08/2011

What specific legal authorities authorize this program or system:

Title 38, United States Code, Sections 501 (b) and 304.

What is the expected number of individuals that will have their PII stored in this system:

1,000,000 - 9,999,999

Identify what stage the System / Application / Program is at:

Operations/Maintenance

The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.

7 years

Is there an authorized change control process which documents any changes to existing applications or systems?

Yes

If No, please explain:

Has a PIA been completed within the last three years?

Yes

Date of Report (MM/YYYY):

11/2010

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

☒ Have any changes been made to the system since the last PIA?

☐ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?

☒ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?

☒ Does this system/application/program collect, store or disseminate PII/PHI data?

☒ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system, please complete TAB 7 & TAB 12. (See Comment for Definition of PII)

2. System Identification

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

Yes

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):

24VA19 : 121VA19 :

2. Name of the System of Records:

3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

24VA19 : Patient Medical Records - VA 121VA19
National Patient Databases - VA 18428 Federal Register
/ Vol. 69, No. 67 / Wednesday, April 7, 2004 / Notices
24VA19: 18435 Federal Register / Vol. 69, No. 67 /
Wednesday, April 7, 2004 / Notices 121VA19
http://www.vhaco.va.gov/privacy/Update_SOR/SOR24VA19.pdf
http://www.vhaco.va.gov/privacy/Update_SOR/SOR121VA19.pdf

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

No

Is PII collected by verbal methods?

No

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

No

Proximity and Timing: Is the privacy notice provided at the time of data collection? Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

No

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

No

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

No

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
-----------	-------------------	--	---------------------------------------	-----------------------------------

Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)		A limited amount of personal information will be collected to allow unique patient identification in the HDR. These data elements include: Name, Sex, Date of birth, Marital status, Race, Ethnicity, Religious preference, Social Security Number, Address, Phone number - residence and work, Mother's maiden name, Date of death, Integration control		
	Electronic/File Transfer	number		

Family Relation (spouse, children, parents, grandparents, etc)	Electronic/File Transfer	Information on the spouse, surviving spouse, and children of veterans who have applied for health beneficiary.		
--	--------------------------	--	--	--

Service Information

Minimal service information will be collected in the HDR. This will be limited to service information included in text-based documents where the veteran's military history is considered important to the treatment of the patient. This may include information on areas where they served, exposure to agent orange or radiation, service-connected conditions, combat experience, etc. Some of this information will also be included in compensation and pensions examination reports.

Electronic/File Transfer

The HDR will store medical information collected on veterans. The clinical domains include: Allergies/Adverse Reactions; Audiology & Speech Pathology; Clinical Decision Support; Clinical Procedures and Medicine; Compensation and Pension Exams; Consultations; Demographics (see above); Dental; Encounters; Event Capture; Health Factors; Home-Based Primary Care; Immunizations/Skin Tests; Laboratory; Mental Health; Nursing; Nutrition and Food Service; Orders; Patient Education; Pharmacy; Problems; Prosthetics; Radiology; Resident Assessment Instrument/Minimum Data Set; Registries; Surgery; Text Documents; Visual Impairment/Blind Rehab; Vitals; Women's Health. This information will be used for clinical decision-making, enhanced patient safety, research studies, population-based reports, bio-surveillance, disease outbreaks, and continuity of care with other healthcare providers veterans may utilize (i.e., Department of Defense, community physicians, specialty laboratories).

Medical Information

Electronic/File Transfer

laboratories).

Criminal Record Information

Guardian Information

Education Information
Benefit Information

Electronic/File Transfer

Patient educational information will be collected and made available to clinicians when treating these patients. This will help veterans and their caregivers understand their medical conditions and alert them to signs and symptoms that may require future treatment.

Other (Explain)

Electronic/File Transfer

Rehabilitation information will be collected from veterans being treated in special programs. Rehabilitation programs are established to treat veterans who have suffered certain injuries and conditions. Injuries and conditions that qualify include head injuries, spinal cord injuries, strokes, cardiac conditions, blindness, post traumatic stress disorders, alcohol and drugs, amputees, etc. Functional independence and outcomes measurements will also be collected.

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal				
Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)		
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)		
Service Information	Yes	VA Files / Databases (Identify file)		
Medical Information	Yes	VA Files / Databases (Identify file)		
Criminal Record Information	No			
Guardian Information	No			
Education Information	No			
Benefit Information	No			
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2011) PLA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization					
<p>The data in the HDR will be retrieved from existing Vista files and organized in a format that supports the delivery of care, regardless of the patient's location or where he has been treated in the past. HDR serves five main purposes: 1. Serve as a primary source for the legal medical record, 2-Enable the generation of clinical reports based on the entire clinical holdings of VHA, 3- Serve as a platform for a re-engineered CPRS, 4- Serve as a platform for patient self-access to the medical record, and 5- Support standardization through the creation of a standards-based database.</p>					
<p>Authentication and authorization are provided Both PII & through the client PHI application.</p>					
<p>Department of Veterans Affairs Vista Databases</p>					
<p>Yes</p>					
<p>Other Veteran Organization</p>					

Other Federal Government Agency

			Clinical Data from the Department of Defense's Clinical Data Repository (CDR) is being shared and stored in the HDR on Active Dual Consumer patients and discharged from the military through the CHDR project (DoD Clinical/VVA Heald Data Repository). This includes patients primarily treated by the VA after discharge or those veterans eligible to be dual consumers of both VA and DoD medical facilities. This currently includes only demographics, outpatient pharmacy and allergies information. Additional data will be shared in the future, but those domains haven't been identified yet. This data will be used for patient treatment and clinical decision-making.	Authentication and authorization are provided Both PII & through the client PHI application.
State Government Agency	Yes	No		
Local Government Agency	No	No		
Research Entity	No	No		
Other Project / System	No	No		
Other Project / System	No	No		
Other Project / System	No	No		

(FY 2011) PIA: Access to Records

5. Data Sharing & Access

Does the system gather information from another system?

Yes

Please enter the name of the system:

Department of Defense, Vista

Per responses in Tab 4, does the system gather information from an individual?

No

If information is gathered from an

☐ Through a Written Request

individual, is the information provided:

☐ Submitted in Person

☐ Online via Electronic Form

Is there a contingency plan in place to process information when the system is down?

Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?

Yes

☐ Drug/Alcohol Counseling

☐ Mental Health

☒ HIV

☒ Research ☐ Sickle Cell ☒ Other (Please Explain)

secondary uses of patient information are specified in the Privacy Act of 1974.

If yes, please check all that apply:

Describe process for authorizing access to this data.

Answer: Electronic file transfer and Computer transfer device. Current information collected in the Health Data Repository is either being extracted directly from the Vista databases (HDR-HX) or being transmitted via HL7 electronic transmissions (HDR-IMS).

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: The VHA, Health Information Management group reviews and approved the content of the database limiting it to only the data required.

How is data checked for completeness?

Answer: Stringent SOA and IV&V processes implemented ensure that data and processed properly. Data checked for completeness is done at the application level and not at the HDR database level.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Source applications are coded to send updates to the database in real time.

How is new data verified for relevance, authenticity and accuracy?

Answer: Addressed at the Vista application level and not at the HDR database level.

Additional information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: The HDR retention process is based upon the Department of Veterans Affairs Record Control Schedule 10-1, Revised June 28, 2006. Data will be retained in the HDR until 3 years after last episode of care. It will then be converted to an archived system but will be retrievable if/when the patient returns for further treatment. Data in the archived system will be retained 75 years after the veteran's last episode of care.

Explain why the information is needed for the indicated retention period?

Answer: Department of Veterans Affairs Record Control Schedule 10-1, Revised June 28, 2006, specifies how long patient data will be maintained.

What are the procedures for eliminating data at the end of the retention period?

Answer: Data will be purged 75 years after the veteran's last episode of care.

Where are these procedures documented?

Answer: VA HBK 6300.1, Records Management Procedures explains the Records Control Schedule procedures.

How are data retention procedures enforced?

Answer: VA Directive 6300, Records and Information Management contains the policies and responsibilities for VA's Records and Information Management program. VA Handbook 6300.1, Records Management Procedures, contains mandatory procedures for the proper management of records effectively and efficiently throughout their life cycle. Neither the directive or handbook is a Records Control Schedule. Procedures are enforced by Records Management Staff and VA Records Officers.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

Information pertaining to TAB 4, Lines (7, 9, 11, 13, 19, 23, 31, 33, 35, 37), Columns D & E:
Information is not obtained directly from Veterans, therefore, data collection comments and
privacy inquiries are not applicable.

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	Automated Medical Information Exchange II (AMIE II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performance Elements Nationwide (ASPEN)
Awards	Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARs)
Awards	Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Braun (CP Hemo)	Control of Veterans Records (COVERS)	Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wireless Messaging System (Blackberry)
Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMII)
Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
IGY Home Loans	IGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
IGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitlement Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Assistant	Service Member Records Tracking System
Omniceil	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
Right Now Web	Rating Board Automation 2000 (RBA2000)	VA Online Certification of Enrollment (VA-ONCE)
SAISHA	Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program
Script Pro	Records Locator System	Veterans Appeals Control and Locator System (VACOLS)
SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sidexis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

VBA Data Warehouse	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		Work Study Management System (WSMS)

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Groupers	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINO	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Management Support
MICOM	MyHealthEver	Health Level Seven	Master Patient Index Vista
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
PAID	Patch Module	MCCR National Database	Pharmacy Benefits Management
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	Progress Notes	Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Verified Components - DSSI
VBECs	VistaLink Security	Text Integration Utilities	Vendor - Document Storage Sys
VDEF	Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistaLink		Voluntary Timekeeping	Voluntary Timekeeping National

Explain any minor application that are associated with your installation that does not appear in the list above. Please

provide name, brief description, and any comments you may wish to include.

Name	Description	Comments	Is PII collected by this minor application?	Does this minor application store PII?	If yes, where?	Who has access to this data?

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web	ENDSOFT	RAFT
	Enterprise Terminology Server &	RALS
A4P	VHA Enterprise Terminology	
	Services	

(FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.

Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..

Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access?

Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: System undergoes System Authorization (C&A) using applicable NIST, VA, and OIG standards, and utilizes a wide range of both VA and OIG security controls to protect data, media, and the system itself.

Explain what security risks were identified in the security assessment? (*Check all that apply*)

- | | | |
|---|---|--|
| <input checked="" type="checkbox"/> Air Conditioning Failure | <input checked="" type="checkbox"/> Data Disclosure | <input checked="" type="checkbox"/> Hardware Failure |
| <input type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Data Integrity Loss | <input type="checkbox"/> Identity Theft |
| <input type="checkbox"/> Blackmail | <input type="checkbox"/> Denial of Service Attacks | <input checked="" type="checkbox"/> Malicious Code |
| <input type="checkbox"/> Bomb Threats | <input type="checkbox"/> Earthquakes | <input checked="" type="checkbox"/> Power Loss |
| <input checked="" type="checkbox"/> Burglary/Break In/Robbery | <input checked="" type="checkbox"/> Eavesdropping/Interception | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Cold/Frost/Snow | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) | <input checked="" type="checkbox"/> Storms/Hurricanes |
| <input checked="" type="checkbox"/> Communications Loss | <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input type="checkbox"/> Substance Abuse |
| <input checked="" type="checkbox"/> Computer Intrusion | <input checked="" type="checkbox"/> Flooding/Water Damage | <input type="checkbox"/> Theft of Assets |
| <input checked="" type="checkbox"/> Computer Misuse | <input type="checkbox"/> Fraud/Embezzlement | <input type="checkbox"/> Theft of Data |
| <input checked="" type="checkbox"/> Data Destruction | | <input type="checkbox"/> Vandalism/Rioting |

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Access Control | <input checked="" type="checkbox"/> Contingency Planning | <input checked="" type="checkbox"/> Personnel Security |
| <input checked="" type="checkbox"/> Audit and Accountability | <input checked="" type="checkbox"/> Identification and Authentication | <input checked="" type="checkbox"/> Physical and Environmental Protection |
| <input checked="" type="checkbox"/> Awareness and Training | <input checked="" type="checkbox"/> Incident Response | <input checked="" type="checkbox"/> Risk Management |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments | | |
| <input checked="" type="checkbox"/> Configuration Management | <input checked="" type="checkbox"/> Media Protection | |

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer:

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?
(Choose One)

- | |
|--|
| <input checked="" type="radio"/> The potential impact is high if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. |
| <input type="radio"/> The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. |
| <input type="radio"/> The potential impact is low if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals. |

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?
(Choose One)

- | |
|--|
| <input type="radio"/> The potential impact is high if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. |
| <input type="radio"/> The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. |
| <input type="radio"/> The potential impact is low if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals. |

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization?
(Choose One)

- | |
|--|
| <input type="radio"/> The potential impact is high if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. |
| <input type="radio"/> The potential impact is moderate if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals. |
| <input type="radio"/> The potential impact is low if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals. |

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2011) PIA: Final Signatures

Facility Name:

Health Data Repository (HDR)

Name

Phone

Email

Privacy Officer:

Garnett Best

202-461-7474

garnett.best@va.gov

 Digital Signature Block

Information Security Officer:

Larry Skrabut

801-588-5208

larry.skrabut@va.gov

Digitally signed by: Larry Skrabut
DN: CN = Larry Skrabut C = US O = U.S. Government OU = Department of Veterans Affairs
Date: 2010.12.08 12:22:00 -07'00'
Reason: I am approving this document

Digital Signature Block

System/Chief Information Owner:

Joe Gibbons

518-449-0618

joe.gibbons@va.gov

Digitally signed by: Joseph F. Gibbons Jr.
DN: cn=US, o=U.S. Government, ou=Department of Veterans Affairs, email=joe.gibbons@va.gov,
cn=Joseph F. Gibbons Jr.
Date: 2010.12.09 14:00:26 -05'00'

Digital Signature Block

#REF!

#REF!

#REF!

#REF!

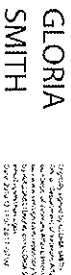
Digital Signature Block

Program Manager:

Gloria Smith

801-588-5052

gsmith@va.gov

 Digital Signature Block

Date of Report:

1/0/00

OMB Unique Project Identifier

029-00-01-11-01-1183-00

Project Name

Health Data Repository (HDR)